FortiAuthenticator - Release Notes

Version 6.2.1

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

April 6, 2022
FortiAuthenticator 6.2.1 Release Notes
23-621-675080-20220406

TABLE OF CONTENTS

Change log

Date	Change Description
2020-11-03	Initial release.
2020-11-23	Updated Hardware VM and Support.
2020-12-01	Information from FortiAuthenticator-VM on page 14 is now available in the VM Install Guide.
2021-04-22	Updated Product integration and support on page 12.
2021-08-11	Updated Product integration and support on page 12.
2021-10-04	Updated Maximum values for VM on page 23.
2021-10-08	Updated Special notices on page 6.
2021-10-19	Updated Maximum values for VM on page 23.
2022-01-04	Updated Upgrade instructions on page 8.
2022-02-24	Updated Maximum values for VM on page 23.
2022-03-03	Added FortiAuthenticator Agent for Microsoft Windows 4.0 and 4.1 to Product integration and support on page 12.
2022-03-23	Updated Product integration and support on page 12.
2022-04-06	Updated Upgrade instructions on page 8.

FortiAuthenticator 6.2.1 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.2.1, build 0552.

FortiAuthenticator is a user and identity management solution that provides strong authentication, wireless 802.1X authentication, certificate management, RADIUS AAA (authentication, authorization, and accounting), and Fortinet Single Sign-On (FSSO).

For additional documentation, please visit: https://docs.fortinet.com/product/fortiauthenticator/

Special notices

TFTP boot firmware upgrade process

Upgrading FortiAuthenticator firmware by interrupting the FortiAuthenticator boot process and installing a firmware image from a TFTP server erases the current FortiAuthenticator configuration and replaces it with factory default settings.

Monitor settings for GUI access

Fortinet recommends setting your monitor to a screen resolution of 1600x1200. This allows for all the objects in the GUI to be viewed properly without the need for scrolling.

Before any firmware upgrade

Save a copy of your FortiAuthenticator configuration before upgrading the firmware. From the administrator dropdown menu in the toolbar, go to **Restore/Backup**, and click **Download Backup File** to backup the configuration.

After any firmware upgrade

Clear your browser cache before logging in to the FortiAuthenticator GUI to ensure the pages display properly.

FortiAuthenticator does not support PEAP-MAB

FortiAuthenticator only supports MAB in clear-text and not the encapsulated MAB.

What's new

FortiAuthenticator version 6.2.1 includes the following new features and enhancements:

LDAP sync rules: email password recovery

This feature introduces the email password recovery option for remote LDAP user sync rules.

When the option is enabled in the sync rule, FortiAuthenticator will:

- Enable the email password recovery setting for new remote LDAP users if they also have a valid email address.
- Enable the email password recovery setting for existing remote LDAP users if they also have a valid email address.

When the option is disabled in the sync rule, FortiAuthenticator will behave the same as in previous releases:

- Disable the email password recovery setting for new remote LDAP users.
- Leave the current email password recovery setting unchanged for existing remote LDAP users.

Upgrade instructions

Back up your configuration before beginning this procedure. While no data loss should occur if the procedures below are correctly followed, it is recommended a full backup is made before proceeding and the user will be prompted to do so as part of the upgrade process.

For information on how to back up the FortiAuthenticator configuration, see the FortiAuthenticator Administration Guide.

Hardware and VM support

FortiAuthenticator 6.2.1 supports:

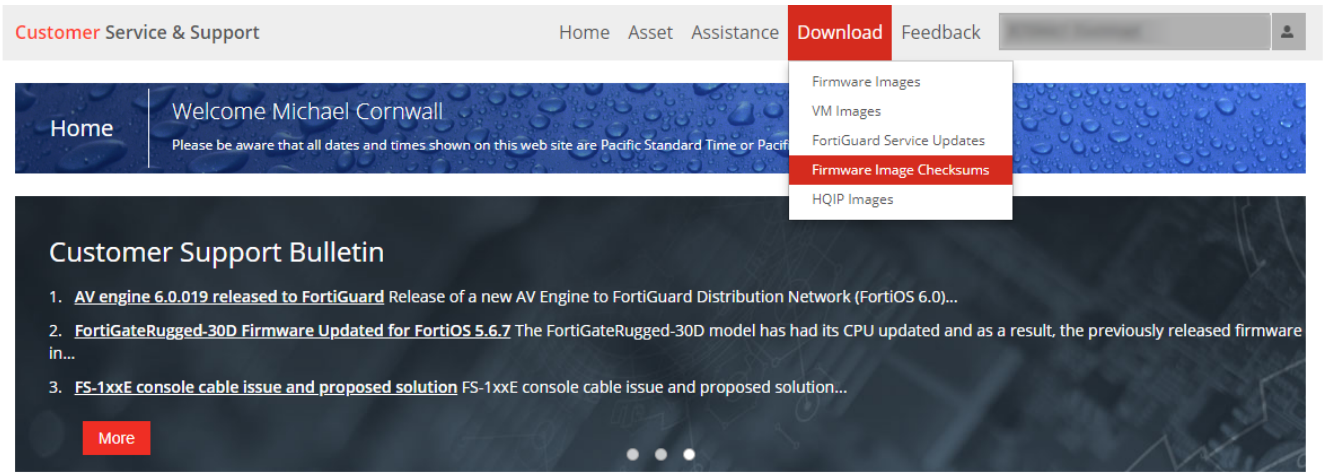
- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator 800F
- FortiAuthenticator VM (VMWare, Hyper-V, KVM, Xen, Azure, AWS, Oracle OCI, and Alibaba Cloud)

Image checksums

To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available from the Fortinet Support website.

Customer service and support image checksum tool



After logging in to the web site, in the menus at the top of the page, click **Download**, then click **Firmware Image Checksums**.

In the **Image File Name** field, enter the firmware image file name including its extension, then click **Get Checksum Code**.

Upgrading from FortiAuthenticator 4.x/5.x/6.x

FortiAuthenticator 6.2.1 build 0552 officially supports upgrades from previous versions by following these supported FortiAuthenticator upgrade paths:

- If currently running FortiAuthenticator 6.0.5 or older, first upgrade to 6.0.7, then upgrade to 6.2.1, else the following message will be displayed: `Image validation failed: The firmware image model number is different from the appliance's.`
- If currently running FortiAuthenticator 6.0.7 or newer, then upgrade to 6.2.1 directly.

When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 6.2.1 from FortiAuthenticator 6.0.7, you must first increase the size of the virtual hard disk drive containing the operating system image (not applicable for AWS & OCI Cloud Marketplace upgrades). See Upgrading KVM / Xen virtual machines on page 10.

Firmware upgrade process

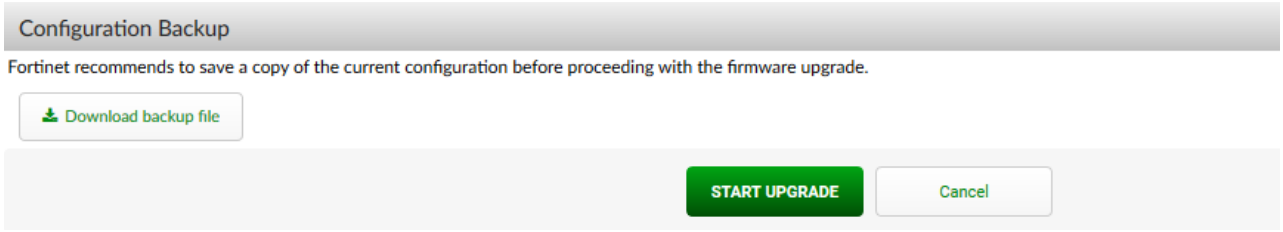
First, back up your configuration, then follow the procedure below to upgrade the firmware.

Before you can install FortiAuthenticator firmware, you must download the firmware image from the Fortinet Support website, then upload it from your computer to the FortiAuthenticator unit.

1. Log in to the Fortinet Support website. In the **Download** section of the page, select the **Firmware Images** link to download the firmware.

2. To verify the integrity of the download, go back to the **Download** section of the login page and click the **Firmware Image Checksums** link.
3. Log in to the FortiAuthenticator unit's web-based manager using the **admin** administrator account.
4. Upload the firmware and begin the upgrade.
   When upgrading from FortiAuthenticator 6.0.4 and earlier:
   a. Go to **System > Dashboard > Status**.
   b. In the **System Information** widget, in the **Firmware Version** row, select **Upgrade**. The **Firmware Upgrade or Downgrade** dialog box opens.
   c. In the **Firmware** section, select **Choose File**, and locate the upgrade package that you downloaded.

   When upgrading from FortiAuthenticator 6.1.0 or later.
   a. Click on the administrator name in the upper-right corner of the GUI to display the dropdown menu, and click **Upgrade**.
   b. In the **Firmware Upgrade or Downgrade** section, select **Upload a file**, and locate the upgrade package that you downloaded.
5. Select **OK** to upload the file to the FortiAuthenticator.
   Your browser uploads the firmware file. The time required varies by the size of the file and the speed of your network connection. When the file transfer is complete, the following message is shown:



   It is recommended that a system backup is taken at this point. Once complete, click **Start Upgrade**.
   Wait until the unpacking, upgrade, and reboot process completes (usually 3-5 minutes), then refresh the page.

Due to a known issue in 6.0.x and earlier releases, the port5 and port6 fiber ports are inverted in the GUI for FAC-3000E models (i.e. port5 in the GUI corresponds to the physical port6 and vice-versa).

This is resolved in 6.1.0 and later, however, the upgrade process does not swap these configurations automatically. If these ports are used in your configuration during the upgrade from 6.0.x to 6.1.0 and later, you will need to physically swap the port5 and port6 fibers to avoid inverting your connections following the upgrade.

Upgrading KVM / Xen virtual machines

When upgrading existing KVM and Xen virtual machines from FortiAuthenticator 6.0.7 to 6.2.1, it is necessary to manually increase the size of the virtual hard disk drive which contains the operating system image before starting the upgrade. This requires file system write-access to the virtual machine disk drives, and must be performed while the virtual machines are in an offline state, fully powered down.

If your virtual machine has snapshots, the resize commands detailed below will exit with an error. You must delete the snapshots in order to perform this resize operation. Please make a separate copy of the virtual disk drives before deleting snapshots to ensure you have the ability to rollback.

Use the following command to run the resize on KVM:

```
qemu-img resize /path/to/fackvm.qcow2 1G
```

Use the following command to run the resize on Xen:

```
qemu-img resize /path/to/facxen.qcow2 1G
```

After this command has been completed, you may proceed with the upgrade from 6.0.7 to 6.2.1

Recovering improperly upgraded KVM / Xen virtual machines

If the upgrade was performed without completing the resize operation above, the virtual machine will fail to properly boot, instead displaying many **initd** error messages. If no snapshots are available, manual recovery is necessary.

To recover your virtual machine, you will need to replace the operating system disk with a good copy, which also requires write-access to the virtual hard disks in the file system while the virtual machines are in an offline state, fully powered down.

To recover an improperly upgraded KVM virtual machine:

1. Download the 6.0.7 GA ZIP archive for KVM, **FAC_VM_KVM-v6-build0059-FORTINET.out.kvm.zip**.
2. Extract the archive, then replace your virtual machine's **fackvm.qcow2** with the one from the archive.
3. Execute the following command:
   `qemu-img resize /path/to/fackvm.qcow2 1G`

To recover an improperly upgraded Xen virtual machine:

1. Download the 6.0.7 GA ZIP archive for Xen, **FAC_VM_XEN-v6-build0059-FORTINET.out.xen.zip**.
2. Extract the archive, then replace your virtual machine's **facxen.qcow2** with the one from the archive.
3. Execute the following command:
   `qemu-img resize /path/to/facxen.qcow2 1G`

Product integration and support

Web browser support

The following web browsers are supported by FortiAuthenticator 6.2.1:

- Microsoft Edge version 86
- Mozilla Firefox version 82
- Google Chrome version 86

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS support

FortiAuthenticator 6.2.1 supports the following FortiOS versions:

- FortiOS v5.4.x and later

Fortinet agent support

FortiAuthenticator 6.2.1 supports the following Fortinet Agents:

- FortiClient v.5.x, v.6.x for Microsoft Windows (Single Sign-On Mobility Agent)
- For FortiAuthenticator Agents for Microsoft Windows and Outlook Web Access compatibility with FortiAuthenticator, see the *Agents Compatibility Matrix* on the Fortinet Docs Library.
- FSSO DC Agent v.5.x
- FSSO TS Agent v.5.x

Other Agent versions may function correctly, but are not supported by Fortinet.

For details of which operating systems are supported by each agent, please see the install guides provided with the software.

Virtualization software support

FortiAuthenticator 6.2.1 supports:

- VMware ESXi / ESX 6.5/6.7/7.0
- Microsoft Hyper-V 2010, Hyper-V 2012 R2, and Hyper-V 2016
- Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0
- Xen Virtual Machine (for Xen HVM)
- Nutanix
- Amazon AWS
- Microsoft Azure
- Oracle OCI
- Alibaba Cloud

Support for HA in Active-Passive and Active-Active modes has not been confirmed on the FortiAuthenticator for Xen VM at the time of the release.

See FortiAuthenticator-VM on page 14 for more information.

Third-party RADIUS authentication

FortiAuthenticator uses standards based RADIUS for authentication and can deliver two-factor authentication via multiple methods for the greatest compatibility:

- RADIUS Challenge Response - Requires support by third party vendor.
- Token Passcode Appended - Supports any RADIUS compatible system.

FortiAuthenticator should therefore be compatible with any RADIUS capable authentication client / network access server (NAS).

FortiAuthenticator-VM

For information about FortiAuthenticator-VM deployments and system requirements, see the VM installation guide on the Fortinet Docs Library.

Resolved issues

The resolved issues listed below may not list every bug that has been corrected with this release. For inquiries about a particular bug, please visit the Fortinet Support website.

Bug ID	Description
612461	Dashes should be allowed in TACACS+ client names.
632033	Unable to change local user password after upgrade - "You do not have permission to perform such operation".
643320	TACACS+: The < and > characters should be allowed for Service name and Attribute name.
659188	GUI does not allow user to edit and save the "Distinguished Name" in LDAP directory tree page.
660309	Extra character (Hex code for backslash) added to the username during LDAP search.
660851	Force password change on next logon produces 403 forbidden with local user after login to self-service or captive portal.
660948	Misbehavior in creating new user group from LDAP directory tree page.
661748	"Authentication Activity" widget shows failed activities which do not exist.
661946	FortiAuthenticator shows "Error 403 Forbidden" when user on LDAP set to "change the password on next login".
665253	During HA cluster failover, remote sync rules do not automatically sync anymore.
665381	CSV MAC device import fails due to MAC address wildcard formatting - MAC address invalid.
665453	Error when trying to backup logs.
665619	Slow GUI in "End Entities - Users" - Gateway Timeout
666236	The login authentication portal no longer provides a way to "log off" on IE with a particular ID after upgrade to 6.1.2.
666293	OAuth token: When authenticating a local user and specifying local realm, a 500 error is shown.
666510	No login prompt for TACACS+ authentication via telnet session.
666892	RADIUS service stopped to authenticate users and user was not able to login to FortiAuthenticator GUI.
668025	FTM provision error after upgrade from version 6.1.2 to version 6.2.0.
668332	Existing RADIUS Policy's Authentication Type lost when adding RADIUS client.
668525	Session expiring when registered to guest portal with MAC parameter enabled.
668747	Unable to give a FTC to a remote RADIUS/SAML user only upon creating the user.
669628	FortiAuthenticator RADIUS server continually crashes if we delete CA certificate being used by RadSec.
669776	Admin with permissions restricted to edit LDAP users only can promote users as FULL ADMIN.
670129	REST API calls against FortiAuthenticator fail with a 500 error.

Bug ID	Description
670768	Unable to update existing, expired certificate - fails with "has expired" but renewed certificate is still valid.
670991	Windows AD Domain Authentication fails to authenticate users; returns NT_STATUS_WRONG_ PASSWORD error.
671144	Unexpected access for admin users with only "Users and Devices" permissions.
671289	TACACS+ service attribute doesn't allow ":" character.
671292	MS-CHAP authentication for local user failed if knowngood password contains "\".
672594	Firmware upgrade fails from 6.1.2 to 6.2.0.
672602	FortiAuthenticator OWA agent stopped working after upgrade to firmware version 6.2.
673547	/auth/ API endpoint returns 401 if password is included in request for remote user authentication.
674190	Two-factor authentication doesn't work for captive self-service portal.

Known issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please visit the Fortinet Support website.

Bug ID	Description
485396	Sponsor/Admin can place created Guest users into any group.
526202	FortiAuthenticator does not check if signature of CSR is valid.
543729	RADIUS client service not working after upgrade.
544691	Remote LDAP admins have no certificate bindings.
566145	Usage Profile "TIME USAGE=Time used" is not triggering COA or disconnect request to FortiGate.
577877	Allow bulk unlock for FTM tokens.
588310	FortiAuthenticator dropping FSSO login events from DC Agent on failed DNS resolution.
588346	An expired certificate is delivered toward WiFi authenticated users.
589219	Multiple DC's kerberos traffic after FortiAuthenticator joining the domain with local DC.
592837	Sponsor accounts can add guest user accounts to non-guest groups.
595012	Should be able to resize the users page column width manually by using mouse.
601520	Recurrent log message: Portal was not found in the session, redirecting back to entry point.
601603	CLI only supports configuring interfaces port1 to port4.
602707	Unable to add multiple alternate DNS names into certificate for user certificates.
604156	Packet captures on OCI seem to be corrupt.
604924	SAML SSO/Proxy metadata download fails with "invalid_xml".
606562	FortiAuthenticator rejects certificate signing requests from FortiGate client with invalid password error.
615442	No Kerberos ticket requests (negotiate) on encrypted HTTPS traffic from FortiAuthenticator.
628815	Remote SAML user import from Azure AD fails Authorization issue.
630041	FortiAuthenticator FSSO - TS Agent sessions stuck at zero after server reboot until FSSOTA service is restarted.
631600	SCEP request by certmonger can't be recognized by automatic enrollment request.
632629	Smart Connect WPA2-Personal profile fails when WPA2-Enterprise settings are left in place.
632637	Smart Connect missing the ability to forget an SSID.
634084	Cannot export third party signed certificate with private key when CSR is generated locally on FortiAuthenticator.
635893	Change password not working with Checkpoint VPN when 2FA is enabled.

Bug ID	Description
637028	SSL connection failed in case of certificate expired error message is not explicit.
637199	Add default usage profiles.
637290	No FTM push notification with Windows agent 3.0.
638374	SCEP - Encryption/hash compatibility with clients.
645043	GUI does not show certificate UPN.
646299	Nutanix AHV KVM based Hypervisor FortiAuthenticator upgrades from 6.0.4 to 6.1.x fails, and hangs on "Waiting for Database".
650215	FortiAuthenticator Windows Agent 3.0 - New RDP connection by the same user is unable to finish due to blank login screen.
652072	When LDAP user password expired, user is not prompted for RSA token code (chained token authentication).
655350	The lockout policy does not apply to username/token submissions to the /auth API endpoint.
657522	SAML authentication fails when AD display name contains a coma (,) and user has admin role.
660357	FSSO FortiGate IP filter ignored when global group prefilter is enabled.
666571	";Portal was not found in the session" when registering a guest with non-ASCII characters "Umlauts".
666636	Wrong group attributes indicator in RADIUS policy response table for EAP-TLS.
666782	If local CA is selected for EAP and no EAP server certificate is present on FortiAuthenticator, radiusd keeps crashing after upgrading to 6.2.0.
666880	GUI - Hide SNMP trap option for PSU monitoring for unsupported devices.
668337	Allowed hosts configuration through CLI is not reflected in GUI before reboot.
668916	Subdomain users can authenticate over FortiAuthenticator Agent installed on workstation in main domain without the token code.
669054	Can't install FAC-VM-HV 6.2.0 on server 2012 R2.
669079	HTTPS certificate chain is inconsistent/incorrect.
670811	Issues with remote SAML user import from Azure AD.
670827	FortiGate filtering stops any users sent to FortiGate even though users are member of group/container.
671345	FortiAuthenticator Windows Agent prompts for token despite incorrect password, and then does not prompt for user credentials again.
672750	When trying to access to self service portal, error "Please enter correct credentials. Note password is case-sensitive" is randomly displayed.
672987	After upgrading FortiAuthenticator from 5.4 to 6.x, Apple devices cannot load the FortiAuthenticator captive portal via the system pop-up only.
673151	Domain controller query status shows failed with successful queries.
673303	Fine-grained menu content has misaligned pointer in SSO/General.

Bug ID	Description
673319	Admin cannot log in to approve the self-registration when group filters are set without admin user in Guest Portal policy.

Maximum values for hardware appliances

The following table lists the maximum number of configuration objects per FortiAuthenticator appliance that can be added to the configuration database for different FortiAuthenticator hardware models.

The maximum values in this document are the maximum configurable values and are not a commitment of performance.

Feature		Model					
		200E	400E	800F	1000D	2000E	3000E
System							
Network	Static Routes	50	50	50	50	50	50
Messages	SMTP Servers	20	20	20	20	20	20
	SMS Gateways	20	20	20	20	20	20
	SNMP Hosts	20	20	20	20	20	20
Administration	Syslog Servers	20	20	20	20	20	20
	User Uploaded Images	39	114	414	514	1014	2014
	Language Files	50	50	50	50	50	50
Realms		20	80	320	400	800	1600
Authentication							
General	Auth Clients (NAS)	166	666	2666	3333	6666	13333
	Users (Local + Remote)[1]	500	2000	8000	10000	20000	40000
	User RADIUS Attributes	1500	6000	24000	30000	60000	120000
	User Groups	50	200	800	1000	2000	4000
	Group RADIUS Attributes	150	150	2400	600	6000	12000
	FortiTokens	1000	4000	16000	20000	40000	80000
	FortiToken Mobile Licenses[2]	200	200	200	200	200	200
	LDAP Entries	1000	4000	16000	20000	40000	80000
	Device (MAC-based	2500	10000	40000	50000	100000	200000

Feature		Model					
		200E	400E	800F	1000D	2000E	3000E
	Auth.)						
	RADIUS Client Profiles	500	2000	8000	10000	20000	40000
	Remote LDAP Servers	20	80	320	400	800	1600
	Remote LDAP Users Sync Rule	50	200	800	1000	2000	4000
	Remote LDAP User Radius Attributes	1500	6000	24000	30000	60000	120000
FSSO & Dynamic Policies							
FSSO	FSSO Users	500	2000	8000	10000	20000	200000[3]
	FSSO Groups	250	1000	4000	5000	10000	20000
	Domain Controllers	10	20	80	100	200	400
	RADIUS Accounting SSO Clients	166	666	2666	3333	6666	13333
	FortiGate Services	50	200	800	1000	2000	4000
	FortiGate Group Filtering	250	1000	4000	5000	10000	20000
	FSSO Tier Nodes	5	20	80	100	200	400
	IP Filtering Rules	250	1000	4000	5000	10000	20000
Accounting Proxy	Sources	500	2000	8000	10000	20000	40000
	Destinations	25	100	400	500	1000	2000
	Rulesets	25	100	400	500	1000	2000
Certificates							
User Certificates	User Certificates	2500	10000	40000	50000	100000	200000
	Server Certificates	50	200	800	1000	2000	4000
Certificate Authorities	CA Certificates	10	10	50	50	50	50
	Trusted CA Certificates	200	200	200	200	200	200
	Certificate Revocation Lists	200	200	200	200	200	200
SCEP	Enrollment Requests	2500	10000	40000	50000	100000	200000

[1] Users includes both local and remote users.

[2] **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

[3] For the 3000E model, the total number of concurrent SSO users is set to a higher level to cater for large deployments.

Maximum values for VM

The following table lists the maximum number of configuration objects that can be added to the configuration database for different FortiAuthenticator virtual machine (VM) configurations.

The maximum values in this document are the maximum configurable values and are not a commitment of performance.

The FortiAuthenticator-VM is licensed based on the total number of users and licensed on a stacking basis. All installations must start with a FortiAuthenticator-VM Base license and users can be stacked with upgrade licenses in blocks of 100, 1,000, 10,000 and 100,000 users. Due to the dynamic nature of this licensing model, most other metrics are set relative to the number of licensed users. The **Calculating metric** column below shows how the feature size is calculated relative to the number of licensed users for example, on a 100 user FortiAuthenticator]-VM Base License, the number of auth clients (RADIUS and TACACS+) that can authenticate to the system is:

100 / 3 = 33

Where this relative system is not used e.g. for static routes, the **Calculating metric** is denoted by a "**-**". The supported figures are shown for both the base VM and a 5000 user licensed VM system by way of example.

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
System					
Network	Static Routes	2	50	50	50
Messaging	SMTP Servers	2	20	20	20
	SMS Gateways	2	20	20	20
	SNMP Hosts	2	20	20	20
Administration	Syslog Servers	2	20	20	20
	User Uploaded Images	19	Users / 20	19 (minimum)	250
	Language Files	5	50	50	50
Authentication					
General	Auth Clients (RADIUS and TACACS+)	3	Users / 3	33	1666

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
User Management	Authentication Policy (RADIUS and TACACS+)	6	Users	100	5000
	Users (Local + Remote)[1]	5	**********	100	5000
	User RADIUS Attributes	15	Users x 3	300	15000
	User Groups	3	Users / 10	10	500
	Group RADIUS Attributes	9	User groups x 3	30	1500
	FortiTokens	10	Users x 2	200	10000
	FortiToken Mobile Licenses (Stacked) [2]	3	200	200	200
	LDAP Entries	20	Users x 2	200	10000
	Device (MAC-based Auth.)	5	Users x 5	500	25000
	Remote LDAP Servers	4	Users / 25	4	200
	Remote LDAP Users Sync Rule	1	Users / 10	10	500
	Remote LDAP User Radius Attributes	15	Users x 3	300	15000
FSSO & Dynamic Policies					

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
FSSO	FSSO Users	5	Users	100	5000
	FSSO Groups	3	Users / 2	50	2500
	Domain Controllers	3	Users / 100 (min=10)	10	50
	RADIUS Accounting SSO Clients	10	Users	100	5000
	FortiGate Services	2	Users / 10	10	500
	FortiGate Group Filtering	30	Users / 2	50	2500
	FSSO Tier Nodes	3	Users /100 (min=5)	5	50
	IP Filtering Rules	30	Users / 2	50	2500
	FSSO Filtering Object	30	Users x 2	200	10000
Accounting Proxy	Sources	3	Users	100	5000
	Destinations	3	Users / 20	5	250
	Rulesets	3	Users / 20	5	250
Certificates					
User Certificates	User Certificates	5	Users x 5	500	25000
	Server Certificates	2	Users / 10	10	500
Certificate Authorities	CA Certificates	3	Users / 20	5	250
	Trusted CA Certificates	5	200	200	200
	Certificate Revocation Lists	5	200	200	200
SCEP	Enrollment Requests	5	Users x 5	500	25000

[1] Users includes both local and remote users.

[2] **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.